

14 MAG 1086

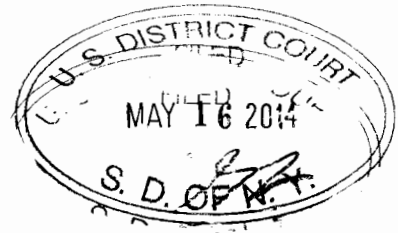
ORIGINAL

Approved: _____

James J. Pastore, Jr.
Assistant United States Attorney

Before: _____

HONORABLE SARAH NETBURN
United States Magistrate Judge
Southern District of New York



----- x
:
UNITED STATES OF AMERICA :
:
- v. - :
:
BRENDAN JOHNSTON, :
a/k/a "BV1," :
:
Defendant. :
:
----- x

SEALED COMPLAINT

Violation of
18 U.S.C. §§ 1030 and 2

COUNTY OF OFFENSE:
New York

DOC # /

SOUTHERN DISTRICT OF NEW YORK, ss.:

PATRICK D. HOFFMAN, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE

(Conspiracy to Commit Computer Hacking)

1. From at least in or about August 2011, up to and including in or about September 2012, in the Southern District of New York and elsewhere, BRENDAN JOHNSTON, a/k/a "BV1," the defendant, and others known and unknown, knowingly and willfully combined, conspired, confederated, and agreed together and with each other to engage in computer hacking, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

2. It was a part and an object of the conspiracy that BRENDAN JOHNSTON, a/k/a "BV1," the defendant, and others known and unknown, knowingly and willfully would and did cause the transmission of a program, information, code and command, and, as a result of such conduct, would and did intentionally cause damage without authorization, to a protected computer, and would and did cause damage affecting 10 and more protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i) and (c)(4)(A)(i)(VI), to wit, JOHNSTON sold malicious software, or

"malware," to others and provided technical support to those using the malware, enabling them to infect and remotely control victims' computers.

Overt Acts

3. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about June 30, 2010, a co-conspirator transmitted a copy of malicious software known as "Blackshades" to an FBI Special Agent located in New York, New York who was acting in an undercover capacity.

b. From at least in or about August 2011, up to and including in or about September 2012, BRENDAN JOHNSTON, the defendant, marketed and sold Blackshades-branded malware through a website that was accessible in the Southern District of New York.

c. In or about 2013, an FBI Special Agent located in New York, New York purchased a copy of malicious software from a website maintained by Blackshades.

(Title 18, United States Code, Section 1030(b).)

COUNT TWO

(Transmission of Malware)

4. From at least in or about August 2011, up to and including in or about September 2012, in the Southern District of New York and elsewhere, BRENDAN JOHNSTON, a/k/a "BV1," the defendant, knowingly and willfully caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, and thereby caused damage affecting 10 and more protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i) and (c)(4)(A)(i)(VI), to wit, JOHNSTON sold, activated, and provided technical support for malware, enabling individuals to infect and remotely control victims' computers.

(Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i) and (c)(4)(A)(i)(VI), and 2.)

The bases for my knowledge and for the foregoing charge are, in part, as follows:

5. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with other law enforcement agents, and my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

6. I have been a Special Agent with the FBI since approximately February 2011. Since approximately February 2012, I have been assigned to a computer intrusion squad in the FBI's New York Field Office. I have received training regarding computer technology, computer fraud, and white collar crimes. I have participated in the arrests of multiple individuals suspected of engaging in cybercrimes.

Overview

7. Since at least in or about 2010, an organization known as "Blackshades" has sold and distributed malicious software to thousands of cybercriminals throughout the world. Blackshades' flagship product was the Blackshades Remote Access Tool, or R.A.T. (the "RAT"), a sophisticated piece of malware that enabled cybercriminals to remotely and surreptitiously gain control over a victim's computer. After installing the RAT on a victim's computer, a user of the RAT had free rein to, among other things, access and view documents, photographs and other files on the victim's computer, record all of the keystrokes entered on the victim's keyboard, steal the passwords to the victim's online accounts, and even activate the victim's web camera to spy on the victim -- all of which could be done without the victim's knowledge.

8. The FBI's investigation has shown that the RAT was purchased by at least several thousand users in more than 100 countries and used to infect more than half a million computers worldwide. The FBI's investigation has included, among other things, the execution of physical search warrants and more than 100 e-mail search warrants, the seizure of more than 1,900 domain names used by purchasers of the RAT to control victims' computers, and the execution of a search warrant for a computer server controlled by Blackshades. Further, an undercover FBI agent in New York, New York obtained a copy of the RAT from one of the RAT's co-creators, who subsequently cooperated with the Government and provided extensive information about Blackshades

("CW-1").¹ The FBI's investigation has revealed that the Blackshades RAT was, in fact, used by Blackshades customers to, among other things, activate web cameras, steal files and account information, and log keystrokes.

9. From in or about August 2011 through in or about September 2012, BRENDAN JOHNSTON, a/k/a "BV1," the defendant, used Blackshades malware and was a paid employee of the Blackshades organization who, among other things, marketed and sold the RAT, and provided technical assistance to users of the RAT to assist them in infecting and remotely controlling victims' computers with the RAT. In certain online postings, JOHNSTON described himself as an "authorized seller" and "admin," or administrator, of Blackshades.

Background on the Blackshades RAT

10. The Blackshades RAT was advertised and discussed, among other places, on online forums for computer hackers. Copies of the RAT were available for sale, typically for \$40 each, on the Blackshades website, which was located at, among other domains, www.blackshades.ru and www.bshades.eu (the "Blackshades Website"). The RAT was typically advertised as a product that conveniently combined the features of several different types of hacking tools. For instance, one online advertisement read:

Deciding between a RAT, a host booter, or
controlling a botnet has never been easier.² With
Blackshades . . . you get the best of all three -

¹ CW-1 was arrested in June 2012 as part of a Government investigation known as "Operation Cardshop." In January 2013, CW-1 pled guilty to two counts of violating Title 18, United States Code, Section 1030 (computer hacking) pursuant to a cooperation agreement with the Government, in the hopes of obtaining a reduced sentence. CW-1 has proven to be reliable, and the information that CW-1 has provided has been corroborated by, among other things, emails and other information seized pursuant to search warrants, as well as logs of online chats seized from CW-1's computer.

² A "host booter" is a tool that can be used to launch a denial of service (or "DoS") attack, typically in the context of online video games. It disconnects or "boots" a person from a "host" (e.g., an online video game platform) and is typically done to cheat at the video game. A "botnet" typically refers to a network of infected computers or "bots."

all in one with an easy to use, nice looking interface.

Even better, Blackshades . . . does a lot of work for you - it can automatically map your ports, seed your torrent for you, and spread through AIM, MSN, ICQ and USB devices.

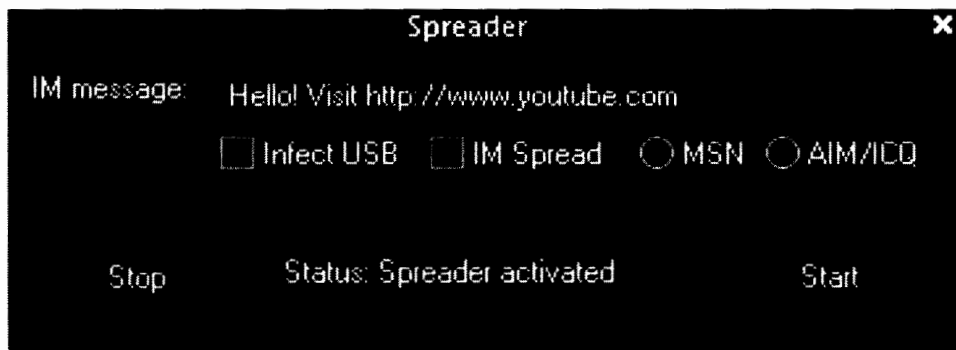
11. Based on my review of the Blackshades software, as well as information provided by CW-1, I know that, after purchasing a copy of the RAT, in order to use it, a user had to install the RAT on a victim's computer - i.e., "infect" a victim's computer. The infection of a victim's computer could be accomplished in several ways, including:

a. by tricking victims into clicking on malicious links contained in emails sent to them;

b. by convincing victims to click on links for videos or to visit websites that caused the malware to be installed; or

c. by hiring others to install the RAT on victims' computers, which at times Blackshades itself offered to do on behalf of its customers for an additional fee.

12. The RAT also contained tools known as "spreaders" that helped users of the RAT infect victim computers. The spreader tools generally worked by using computers that had already been infected to help spread the RAT further to other computers. For instance, as depicted below, in order to lure people to click on malicious links that would install the RAT on their computers, the RAT allowed users to send those malicious links to others via a victim's social media service, making it appear as if the message had come from the victim's compromised computer:

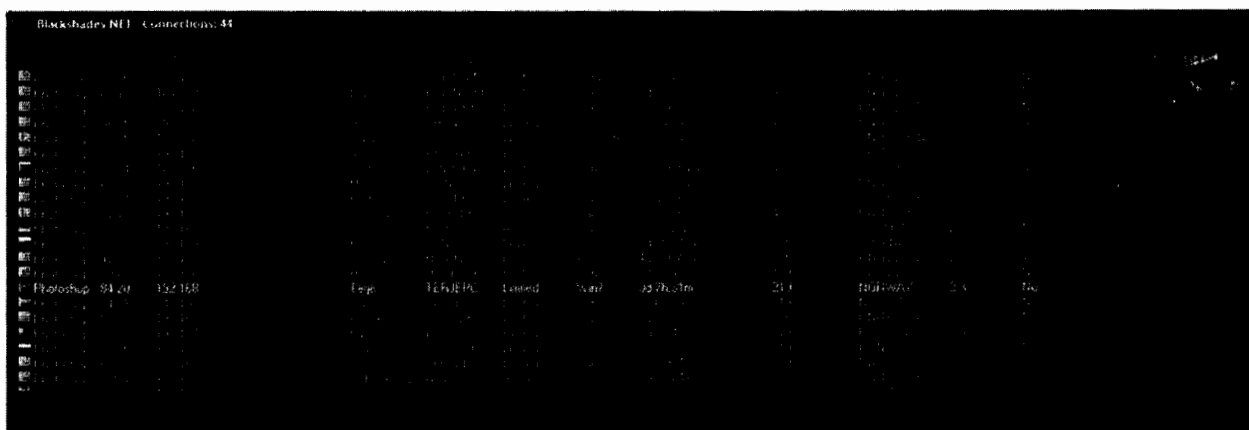


In this example, the user of the RAT has set the RAT to be spread through a malicious link that would be sent to others via

the victim's instant messaging, or IM, services. In this case, the victim's social contacts would receive an IM message (purportedly from the victim), saying "Hello!" and inviting them to click on a link that appeared to lead to the YouTube website. In this way, the victim's friends might be fooled into clicking on the link purportedly sent by the victim, which would in fact install the RAT on that person's computer.

As can be seen above, the RAT's spreader feature also provided users an option to "Infect USB," which would infect any device plugged into a USB port on the victim's computer, such as a thumb drive. In this way, the malware could be spread between two computers through use of a thumb drive (e.g., a person's home and work computers).

13. The RAT also featured a graphical user interface, which allowed cybercriminals to easily view and navigate all of the victim computers that they had infected:



Among other things, the user interface³ listed IP address information for each infected computer, the computer's name, the computer's operating system, the country in which the computer was located, and whether the computer had a web camera.

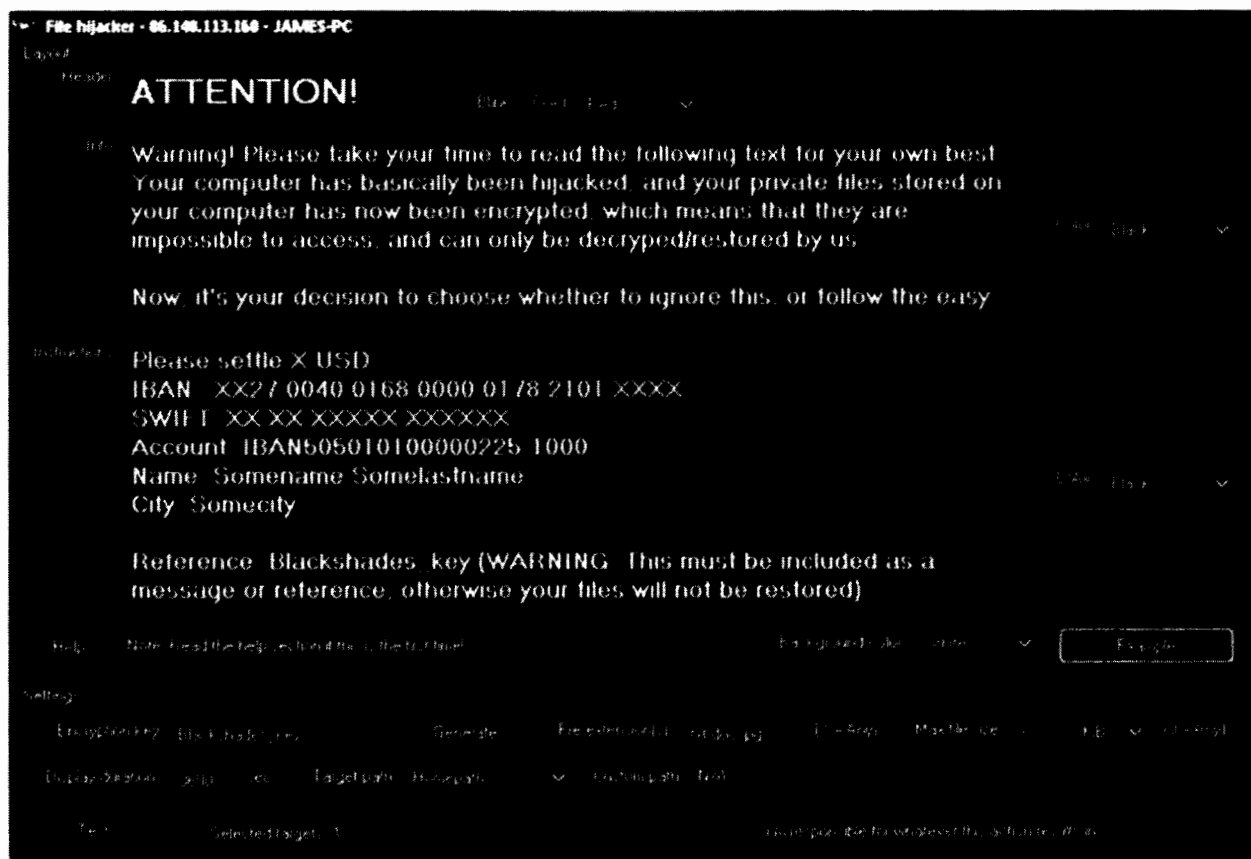
14. Once a computer was infected with the RAT, the user of the RAT could remotely activate the victim's web camera. By doing so, the RAT user could take photographs or obtain a live feed from the infected computer's web camera. In this way, the user could spy on anyone within view of the victim's webcam inside the victim's home or in any other private spaces where the victim's computer was used.

15. The RAT also contained a "keylogger" feature that allowed users to record each key that victims typed on their

³ A copy of the interface is attached hereto as Exhibit A.

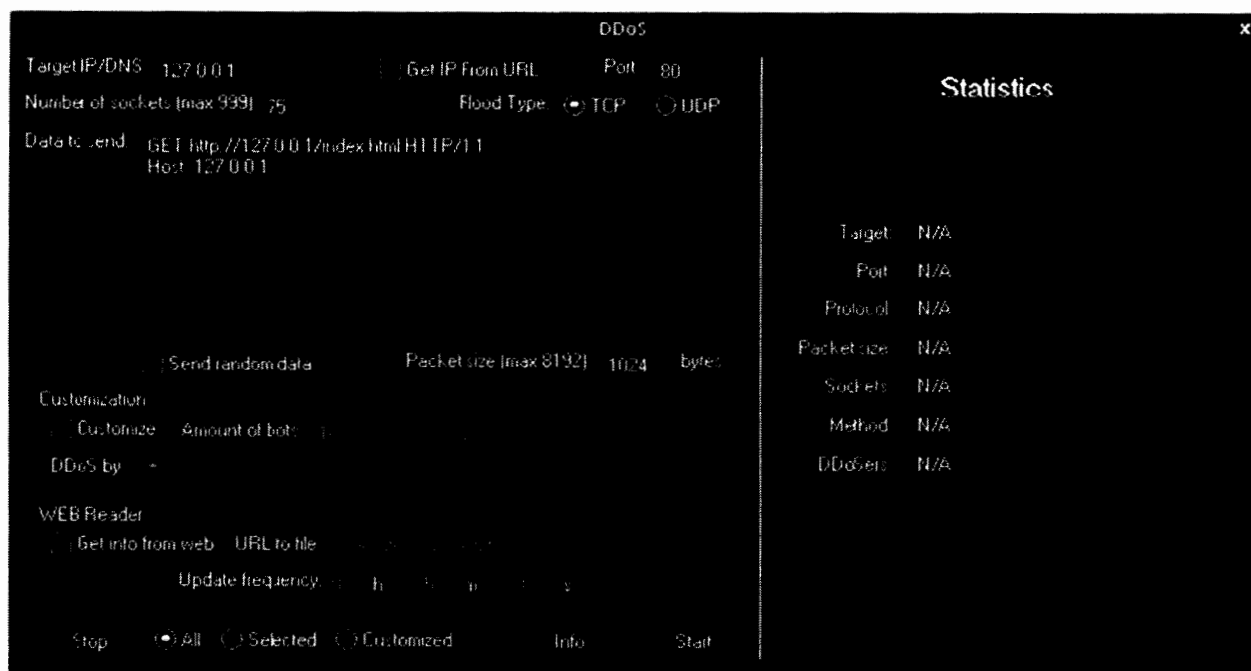
computer keyboards. To help users steal a victim's passwords and other log-in credentials, the RAT also had a "form grabber" feature. The "form grabber" automatically captured log-in information that victims entered into "forms" on their infected computers (e.g., log-in screens or order purchase screens for online accounts).

16. The RAT also provided its users with complete access to all of the files contained on a victim's computer. A RAT user could use such access to view or download photographs, documents, or other files on a victim's computer. Further, using a tool known as "file hijacker," the RAT enabled users to encrypt, or lock, a victim's files and demand a "ransom" to unlock them. This "ransomware" feature of the RAT included a pre-drafted ransom note that could be sent to victims:



17. The RAT also allowed users to exploit victims' computers to launch other cyber attacks. Infected computers - which, as noted above, are sometimes referred to as "bots" - could be gathered into a network known as a "botnet." The botnet could then be used to launch Distributed Denial of Service ("DDoS") attacks against particular websites by repeatedly

sending requests to the website in an effort to disable the website and deny service to legitimate customers. The RAT included a special DDoS tool that simplified the process of launching DDoS attacks using infected computers:



18. The RAT also included several features that were designed to harass or frighten victims. One feature, for example, allowed RAT users to "talk" to a victim through the victim's own infected computer by using the computer's "speech to text" feature. That is, a RAT user could type a message to the victim, and the victim's computer would read the message aloud. Another feature of the RAT caused an online chat window to appear on a victim's computer, through which the RAT user could type messages to the victim. The victim was unable to close, move, or otherwise remove the chat window.

Other Blackshades Products and Services

19. Based on my review of the Blackshades Website, as well as information provided by CW-1, I know that, in addition to the RAT, Blackshades has also sold Blackshades Crypter, a program designed to make the RAT undetectable by anti-virus software; Blackshades Stealth, a version of the RAT coded in certain programming languages that allowed the RAT to be controlled by Macs in addition to PCs; and Blackshades Fusion, malicious software designed to steal passwords, launch DDoS attacks, and capture webcam feeds, among other things.

20. Based on the FBI's review of a server controlled by Blackshades (the "Blackshades Server"), a copy of which was obtained by the FBI pursuant to a search warrant, I know that the Blackshades Server stored usernames and passwords of victims that had been stolen using Blackshades products. A Blackshades customer could access and download to his or her computer the stolen usernames and passwords by logging into his or her Blackshades account.

21. From speaking with CW-1 and from reviewing the Blackshades Website, I also know that from time to time Blackshades has provided a service known as a "Virtual Private Network" or "VPN." Based on my training and experience, I know that VPNs can be used to obscure the true IP address of a computer. Accordingly, cybercriminals often use VPNs to make it more difficult for law enforcement to identify their true IP addresses and physical locations.

The Blackshades Organization

22. Based on information provided by CW-1 and other witnesses, as well as records obtained pursuant to search warrants, I know that Blackshades operated as a business, which was owned and operated by Alex Yucel, a/k/a "marjinz." Among other things, Yucel hired and fired employees, paid employees' salaries, and updated the malicious software in response to customers' comments and requests. To facilitate the operations of the Blackshades organization, Yucel employed several paid administrators, including a director of marketing, website developer, customer service manager, and a team of customer service representatives. In addition to running the Blackshades organization, Yucel - along with CW-1 - created the RAT.

23. Based on my review of the Blackshades Website, information provided by CW-1, and records obtained pursuant to search warrants, I know that Blackshades maintained a customer support forum on its website and had a customer support email address. Customer complaints were opened as "trouble tickets," and would be answered by one of several paid customer service representatives. The Blackshades Server included employee reviews written by Yucel, as well as records reflecting payments made to employees.

24. Records obtained from various electronic payment processors show that Blackshades generated sales of more than \$350,000 between September 2010 and April 2014.

The FBI's Identification of Blackshades Users and Seizure of Domains Used to Control Victim Computers

25. According to information provided by CW-1, customers who wished to use the RAT were required to set up an account with Blackshades that included a username and password. In addition, to deploy the RAT, each Blackshades customer was required to determine how his victims' computers would communicate with his computer. Typically, RAT users set up their accounts so that their victims' computers would communicate with a particular domain name, such as www.example.com. That domain name, in turn, was associated with the IP address of the RAT user's computer through the Domain Name System, or DNS.⁴

26. According to CW-1, when a Blackshades customer set up the RAT, the Blackshades Server logged the domain name to which that customer directed his victims' computers. This information was maintained in one or more database tables on the Blackshades Server. As indicated above, the Government seized a copy of the Blackshades Server pursuant to a search warrant. The copy of that server contained database tables that reflected the usernames and passwords associated with Blackshades accounts, as well as the domain names to which Blackshades users directed their victims' computers.

27. Records obtained from the Blackshades Server and other documents showed that there were more than 6,000 Blackshades customer accounts.⁵ Based on information users provided to Blackshades, those users were located in more than 100 countries.

28. As part of the Government's investigation, the Government obtained a court order authorizing the seizure of more than 1,900 domain names used by certain Blackshades customers to control infected computers. By doing so, the FBI disabled communications between those infected computers and the RAT users that had infected them. The court order also authorized the FBI to obtain IP address information for computers trying to communicate with the seized domain names, to enable the FBI to

⁴ Based on my training and experience, I know that DNS is the system through which an easily memorable domain name (e.g., www.doj.gov) is translated - or "resolved" - into an IP address (e.g., 149.101.1.3), thus allowing information to be transmitted between computers.

⁵ The number of customer accounts does not necessarily reflect the number of unique users because a single user could have maintained multiple accounts.

identify and facilitate notification to victims regarding the infections.

**"BV1" Sells, Administers, and Provides Technical Support
for the RAT**

29. I have reviewed the contents of certain e-mail accounts used by CW-1, pursuant to CW-1's consent, which contain e-mail exchanges between CW-1 and Yucel, including a chain of e-mails between CW-1 and Yucel from March 20, 2012, with the subject line, "Re: Inquiry."

a. The e-mail chain begins with an e-mail from CW-1, who tells Yucel that he is interested in returning to the Blackshades operation. (According to CW-1, he/she left the Blackshades operation temporarily in or about August 2011 but sought to return in March 2012). CW-1 stated:

I have heard that Blackshades sales have gone down since my departure. I don't think this is entirely due to my absence, but I do think that if I were to come back, some people would feel a rejuvenated feeling and wish to consider Blackshades again - especially if I came back on HackForums with my same username and profile. I can offer insight and some expertise in Web Programming fields; something I don't know if your team currently has. I can also try to tackle marketing aspects, because with the reputation blackshades has, there should be many more sales. . . .

b. Yucel responded to the e-mail, stating that he was now mainly working with someone using the moniker "BV1" as his salesperson. Yucel explained that he had worked out an arrangement with "BV1" that allowed "BV1" to keep all revenue from sales executed through certain payment systems, while Yucel was keeping the money from all sales made through a different payment system. Yucel told CW-1, "I'd really love to have you back in the team, but I hope you understand that I don't want to lose money if you get back."

30. I have reviewed various postings on a particular online forum used by computer hackers (the "Forum"), which included messages sent to and from an individual using the username "BV1." Those postings included the following:

a. On or about April 11, 2012, a user of the Forum with the username "BV1" posted an advertisement stating,

"Blackshades is proud to present our newest product: Blackshades Stealth." The advertisement described the features of the product, including "screen capture," "webcam capture," "voice capture," and "keylogger." The advertisement further provided instructions on how to buy the product.

b. On or about October 19, 2011, a user named "sorenm" posted a message to the Forum titled "After Payment to Blackshades no one is activating or replying my mails or PMS [private messages]." In the post, "sorenm" explained that he had paid "BV1 from Blackshades" \$40 "about a week ago" to set up "my account," but that "BV1" had failed to follow through. "sorenm" stated, "Below is the email "BV1" sent me [] 2 days ago." Appended at the end of the post is an e-mail from "Brendan" at the e-mail address "bmjslider@yahoo.com" (the "BV1 Email Account"). In the e-mail, "BV1" apologized for the delay in responding to "sorenm," explaining that there had been an emergency in his family and that he would be "back to work roughly 12 hours from now."

c. On or about September 25, 2012, "BV1" made a post on the Forum stating, "[W]e've just recently sold our 6,000th copy of our RAT" and that "we've just recently hit our 20,000th customer in total." The post further stated that anyone who sent "BV1" a private message would receive "\$10 off their RAT order, and \$5 off of any other product[] that Blackshades has to offer." The post included a logo for "BV1" describing him as "Blackshades BV1" and indicating that he was an "Official Seller and Admin[istrator]" of Blackshades.

31. On or about October 12, 2012, the FBI obtained a search warrant for the BV1 Email Account. Among other emails seized pursuant to the search warrant were the following:

a. An email dated June 7, 2012 whose "From" field indicated that it was sent by "Brendan Johnston <bmjslider@yahoo.com>" which stated, in part, "I have activated your RAT." The email also provided a username and password for the recipient's Blackshades account, and provided directions for how the recipient could access the Blackshades account through a website then-located at bshades.eu/myservices.php.

b. An email dated February 2, 2012 whose "From" field indicated that it was sent by "Brendan <bmjslider@yahoo.com>," which provided directions to the recipient for sending payment for the RAT.

c. Multiple emails consisting of records of payments made through an electronic payments processor from an account

called "Blackshades" to an account in the name of "Bmjslider," which appear to reflect payments to JOHNSTON for his work with the Blackshades organization. For example, one of the records indicated that the payment constituted the "administrator share." As noted above, in posts on the Forum, "BV1" identified himself as an official administrator and seller of Blackshades.

d. An email dated February 19, 2011 addressed to "Brendan" containing a receipt reflecting his purchase of the Blackshades RAT.

32. According to CW-1, "BV1" was hired in CW-1's absence to, among other things, market and manage sales for Blackshades malware. Moreover, Yucel told CW-1 that Yucel paid "BV1" a monthly fee and that "BV1," in turn, paid members of a support team who assisted with the administration of Blackshades malware.

33. My review of records obtained from the Blackshades Server further confirm that "BV1" served as an administrator for Blackshades. Among other files contained on the Blackshades Server was one titled "Staff_Log," which contained a log of actions taken by various employees of Blackshades. There are several entries associated with "BV1," indicating that "BV1" added, removed, and updated Blackshades user accounts associated with the RAT.

Identification of BRENDAN JOHNSTON, the Defendant, as "BV1"

34. The investigation has revealed that "BV1" is in fact BRENDAN JOHNSTON, the defendant. As noted above, emails contained in the BV1 email account indicate that they were sent to or received from "Brendan Johnston" or "Brendan."

35. Another email contained in the BV1 Email Account reflected an order from Amazon.com that was sent to "Brendan Johnston" at a particular address in Thousand Oaks, California (the "JOHNSTON Address").

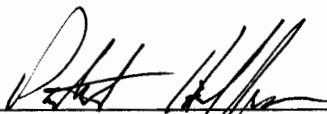
36. Records obtained from Yahoo! indicate that the BV1 Email Account was accessed from a particular IP address on several occasions in or about September 2012. The subscriber records for that IP address obtained from the Internet Service Provider indicate that, as of September 2012, the IP address was assigned to "Christopher [sic] Johnston" at the JOHNSTON Address in Thousand Oaks, California.

37. California Department of Motor Vehicle records indicate that BRENDAN JOHNSTON, the defendant, resided at the JOHNSTON Address as of May 2010. In or about April 2014, FBI


agents in California conducted surveillance at the JOHNSTON Residence and observed in the garage of the Residence an individual who appeared to be the same person depicted in JOHNSTON's driver's license photograph.

38. Further, I have reviewed an online posting to a service known as Pastebin that identified "BV1" as BRENDAN JOHNSTON, the defendant, and listed the JOHNSTON Address as his home address and bmjslider@yahoo.com as his email address. (This type of activity is sometimes referred to as "doxing" an individual - that is, putting their personal information or "documents" online.) The BV1 Email Account contained an email to Pastebin dated September 20, 2012 confirming that the posted information was accurate, and requesting that Pastebin remove the post containing JOHNSTON's personal information.

WHEREFORE, I respectfully request that an arrest warrant be issued for BRENDAN JOHNSTON, a/k/a "BV1," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.


PATRICK D. HOFFMAN
Special Agent
Federal Bureau of Investigation

Sworn to before me this
16th day of May 2014


HON. SARAH NETBURN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

